Addendum to September 20, 2013 Submission to the Secretary of the Navy from the Assistant Secretary of the Navy (Manpower and Reserve Affairs)

Background

This addendum supplements the initial findings and recommendations of the Assistant Secretary of the Navy (Manpower and Reserve Affairs) (ASN (M&RA)) regarding the service record, performance evaluations, and security clearance history of former Sailor Aaron Alexis. Additionally, ASN (M&RA) reviewed whether the Department of Navy (DON) followed all applicable rules and processes concerning the granting and maintaining of his security clearance when Alexis was a contractor employee. The supplemental findings which are germane to each of these tasks are contained below.

Timeline of Service Record, Performance Evaluations, and Security Clearance History

Our review of Alexis's service record, performance evaluations, and security clearance history was designed to determine the degree to which his conduct on and off duty in the Navy did or did not meet the requirements for eligibility for a security clearance and fitness for duty. The rapid review accomplished this tasking by examining Alexis's background from approximately three years prior to his enlistment through the date that he was discharged from the Navy.

The timeline on pages 3-4, dated November 1, 2013, outlines the events from approximately three years prior to his enlistment up through the issuance of his Navy Reserve Identification and Privilege card on February 22, 2011.

Subsequent to Alexis's discharge from the Navy, according to Defense Security Service (DSS) records, a company called "The Experts" employed him as a contractor on two separate occasions. The first period was September 5, 2012, to December 21, 2012; the second began July 8, 2013. Based on his employment with The Experts, Alexis was issued a DoD Contractor Identification card on July 11, 2013, with an expiration date of July 3, 2016. According to DSS, The Experts' Facility Security Officer validated Alexis's eligibility for a security clearance without ordering a new background investigation because he was released from active duty less than 24 months prior to the date that he was hired with The Experts. Additionally, no security clearance background investigation was required during his subsequent employment because it was within 24 months of the termination of his first term of employment with the company. Alexis's eligibility to maintain a security clearance was valid until March 10, 2018.

Lastly, according to Alexis's Joint Personnel Adjudication System (JPAS) record, The Experts removed his access to Secret information on August 7, 2013. However, on August 9, 2013, The Experts restored his access to Secret information. Despite The Experts' decision to temporarily remove his access to Secret information, Alexis's JPAS record does not contain any information from The Experts stating why the company took this action.

Finding

Given the information available to the Navy regarding Alexis's pre-service conduct, coupled with his conduct not meeting the serious/significant threshold, as assessed by his squadron during the term of his enlistment, he met the requirements for eligibility for a security clearance and continued service in the Navy.

Did the DON follow all the rules and processes concerning the granting and maintaining of Alexis's security clearance when he was a contractor employee?

Our review of the rules and processes concerning the granting and maintaining of security clearances was designed to determine whether the DON followed all applicable rules and processes concerning the granting and maintaining of Alexis's security clearance when he was a contractor employee.

Finding

During his employment with The Experts, the company was responsible for ensuring that Alexis maintained his eligibility for a security clearance in accordance with standard Continuous Evaluation criteria in compliance with the National Industrial Security Program Operating Manual. The Experts were required to report any behavior or conduct that was detrimental to security to the Department of Defense Consolidated Adjudicative Facilities via the DSS. The rapid review did not reveal any adverse information reports regarding Alexis; however, the recently ordered investigation in accordance with the Manual of the Judge Advocate General will determine whether adverse information notifications were made and whether all applicable reporting requirements were complied with in relation to Alexis. See TAB B.

Recommendations

Our recommendations remain unchanged from the initial recommendations provided to the Secretary on September 20, 2013:

- Require Command Security Manager responsibilities be assigned to Executive Officers or other senior member of the Command leadership team vice the current practice of assigning these duties to junior officers.
- Require senior-level accountability on all detachment of individual evaluations/fitness reports.
- Recommend all Office of Personnel Management investigative reports include any available police documents related to the subject being investigated for clearance eligibility.

Pursuant to a Secretary of the Navy memorandum dated September 24, 2013, the Chief of Naval Operations and Commandant of the Marine Corps, with the assistance of the Assistant Secretary of the Navy (Manpower and Reserve Affairs), have been directed to determine the implications of implementing the first two of these recommendations. The third recommendation has been forwarded to the Secretary of Defense for action as deemed appropriate.

November 1, 2013

Subj: TIMELINE OF EVENTS CONCERNING AARON ALEXIS
****

1. On June 3, 2004, approximately three years prior to his enlistment, Aaron Alexis was arrested in Seattle, WA for a May 5, 2004 incident. He was charged with malicious mischief, remained in jail overnight, and released on his own recognizance. No charges were formally filed.

2. On May 5, 2007, Alexis enlisted in the Navy Reserve at New York Military Entrance Processing Station, Brooklyn, NY.

3. Upon Alexis's entry into the Navy, the standard background investigation request via the Standard Form 86 (SF 86 – National Security Questionnaire) for a Secret level clearance, or National Agency Check with Law and Credit Check, was submitted to the Office of Personnel Management (OPM), DoD's Investigative Service Provider. Based on a fingerprint check with the FBI's Criminal Justice Investigation System and a Washington statewide check of district and municipal courts information, OPM became aware of the June 3, 2004 arrest for Malicious Mischief in Seattle, WA. As a result, OPM conducted a subject interview with Alexis due to his omission of the 2004 arrest on his SF 86. OPM closed its investigation on August 24, 2007. Since the Washington statewide check did not reflect that a firearm was used, the resulting report to the Department of Navy Central Adjudication Facility (DONCAF) did not include any mention of the use of a firearm in the 2004 Seattle incident. During the interview that OPM conducted of Alexis, Alexis described an incident in which he "deflated the tires on a construction worker's vehicle."

4. On July 10, 2007, Alexis graduated from Recruit Training in Great Lakes, IL. On December 15, 2007, he graduated from Aviation Electrician's Mate "A" School and transferred to Fleet Logistics Support Squadron 46 in Atlanta, GA. Alexis remained with this squadron for his entire time in the Navy. Due to Base Realignment and Closure, the squadron relocated to Fort Worth, TX in 2009.

5. On March 11, 2008, DONCAF, upon review of the OPM investigation, determined Alexis was eligible for a Secret level security clearance, with a single caution to the squadron concerning his negative credit history. At the time of Alexis's investigation and adjudication, a Secret level clearance was good for 10 years.[1]

6. On September 23, 2008, then Commander (now Captain) [redacted] imposed non-judicial punishment (NJP) on Alexis for Unauthorized Absence (Article 86, Uniform Code of Military Justice (UCMJ)). He received forfeiture of 1/2 pay per month for 2 months (suspended) and was reduced one pay grade (suspended). The reason for the unauthorized absence was that Alexis was in jail from August 10-11, 2008 in DeKalb County, GA following an arrest for disorderly conduct outside of a nightclub. The Record of NJP appears in his service record from this date forward.

7. On July 12, 2009, Commander [redacted] imposed a second NJP on Alexis for being drunk and disorderly (Article 134, UCMJ). He was reduced one pay grade. This NJP was due to Alexis leaping off stairs and breaking his ankle while reportedly intoxicated. There was no police involvement. Alexis appealed this NJP.

---

[1] In 2012, the Directors of National Intelligence and Office of Personnel Management ordered periodic reinvestigations for individuals cleared at the Secret level to be completed every five years. DoD anticipates this new requirement will be implemented in 2015, at the earliest.

8. Commander (b) (6), (b) (7)(C) (now Captain) assumed command of the squadron on August 16, 2009.

9. On December 3, 2009, pursuant to Alexis's appeal, Commander (b) (6), set aside the NJP based on a finding that there was insufficient evidence to prove he was intoxicated at the time of the incident.[2] The Report of NJP was removed from his record.

10. On September 5, 2010, Alexis was arrested in Fort Worth, TX for discharging a firearm in his residence the previous day. According to law enforcement documents, Alexis stated he accidentally discharged the firearm while cleaning it. No charges were filed.

11. Subsequent to Alexis's arrest in Fort Worth, TX, Commander (b) (6), began the process to administratively separate him from the Navy. Specifically, Commander (b) (6), 's legal officer prepared an administrative separation document that he intended to forward to Navy Personnel Command. However, after Alexis was not charged for unlawfully discharging a firearm, this document was not signed, dated or sent.

12. Alexis had no security incidents reported in the Joint Personnel Adjudication System.[3]

13. The United States Navy has no record of any civilian conviction of Alexis.

14. On December 2, 2010, Alexis requested separation from the Navy in accordance with the existing "Reduction in Force" program allowing Sailors to request an early release from the Navy.

15. On December 9, 2010, Navy Personnel Command approved the member's request for separation. On January 31, 2011, he received an Honorable discharge with a Reentry Code of RE-1, the most favorable code.

16. Alexis was issued a Navy Reserve Identification and Privilege card on February 22, 2011 with an expiration date of May 4, 2015.

[2] Commander (b) (6), was verbally informed by the appeal authority, Commander, Naval Air Force Reserve, that upon his review of Alexis's appeal, based on a lack of evidence regarding Alexis's intoxication, he would set aside the NJP if Commander (b) (6), did not set it aside on his own.

[3] The Joint Personnel Adjudication System is used extensively by the Department of Defense Central Adjudicative Facilities (DODCAF) to record information affecting individual eligibility to access classified information. In 2013, the individual Service Adjudicative Facilities merged and became DODCAF.

Contractor Security Clearances:
Process, Requirements, and Recommendations

This rapid review addresses the current processes and requirements for contractors and their employees to maintain a security clearance, including any requirement for notification to the appropriate federal authority of derogatory and adverse information concerning their employees. The review recommends changes to the existing processes and requirements, as well as areas for in-depth review as part of the recently ordered investigation under the Manual of the Judge Advocate General (JAGMAN investigation). In addition, this review evaluates how the current processes and requirements were implemented under the Continuity of Service Contract (CoSC) which was awarded to Hewlett Packard Enterprise Services, LLC (HPES) on July 8, 2010, and under a subcontract on which Aaron Alexis was hired.[1]

Recommendation 1 – Clarify Acquisition Regulations Regarding Inclusion of Security Requirements in Department of the Navy (DON) Contracts

- In the near term, the Navy/Marine Corps Acquisition Regulation Supplement (NMCARS) should be updated to require specifically that contracting officers shall include clause 52.204-2 in commercial item and commercial services contracts, as applicable under FAR Subpart 4.4. The Assistant Secretary of the Navy (Research, Development and Acquisition) (ASN (RD&A)) should conduct a review of all existing commercial item contracts to determine if they involve access to classified information, and if so, modify the contracts to add FAR 52.204-2 and any other applicable security requirements. This modification would likely increase the cost of existing contracts.

- In the long term, the General Counsel of the Navy (General Counsel) and ASN (RD&A) should be directed to prepare a proposed amendment to the FAR and/or DoD FAR Supplement (DFARS) that would implement this improvement more broadly in Government contracting and submit it to the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD (AT&L)) for consideration.

Background

Executive Order (EO) 12829, Jan. 6, 1993 (58 Fed. Reg. 3479, Jan. 8, 1993), establishes a program to safeguard Federal Government classified information that is released to contractors, licensees, and grantees of the United States Government. EO 12829 amends previous EOs that govern safeguarding classified information within industry. The National Industrial Security Program Operating Manual (NISPOM), DoD 5220.22M, and Industrial Security Regulation, DoD 5220.22R, implement the program that is required by EO 12829.

[1] Contract No. N00039-10-D-0010. The Department of the Navy (DON) awarded the Continuity of Service Contract (CoSC) to Hewlett Packard Enterprise Services, LLC (HPES) on July 8, 2010, for continuing provision of Navy Marine Corps Intranet (NMCI) services to the DON pending award and transition of services to the Next Generation Enterprise Network (NGEN) contract.

With respect to DON contractors and their employees, the Federal Acquisition Regulation (FAR) requires contracting officers to include a clause entitled "SECURITY REQUIREMENTS (AUG 1996)," FAR 52.204-2, in solicitations and contracts "when the contract may require access to classified information." FAR 4.404(a). The clause requires the contractor to comply with, among other things, the requirements of the NISPOM, and to include "terms that conform substantially to the language of this clause . . . in all subcontracts . . . that involve access to classified information." FAR 52.204-2(d). In addition, contracting officers shall inform contractors and subcontractors of the security classifications and requirements under the contract using the DoD Contract Security Classification Specification (DD Form 254). FAR 4.403(c). The DD Form 254 is approved by the contracting officer or the contracting officer's authorized representative, *e.g.*, a security contracting officer representative. *Id*.

Chapter 7 of the NISPOM describes a prime contractor's responsibilities when disclosing classified information to a subcontractor. The prime contractor is required to determine the security requirements of the subcontract, determine clearance status of prospective subcontractors, and ensure that a Contract Security Classification Specification is incorporated in each classified subcontract. Prime contractors are advised that they may extract pertinent information from a variety of sources, including the Prime contract DD Form 254, in creating the subcontract DD Form 254.

The rapid review revealed, based on a limited survey of contracts, that while the requirements are incorporated into most contracts, there is a potential for the applicable clauses to be omitted from commercial item contracts based on the FAR provision and clause matrix (FAR Matrix), FAR 52.301. The FAR Matrix requires that clause 52.204-2 be included in all types of contracts, as applicable, *with the exception of* commercial item contracts issued under FAR Part 12.[2]

Application of Processes and Requirements to the CoSC Contract

CoSC is a commercial item contract which was issued under FAR Part 12, for which the FAR Matrix does not require inclusion of clause 52.204-2. Generally, contracts for commercial items under FAR Part 12 only include those clauses required to implement provisions of law or executive orders applicable to the acquisition of commercial items.[3] In addition, FAR Part 12 contracts may include additional clauses, if the contracting officer determines that the additional clauses are consistent with customary commercial practice.[4] The contracting officer should not include additional clauses, even if they are required by prescriptions in other FAR parts, unless the clauses fall into one of these two categories. With respect to CoSC, the contracting officer determined that the provisions of FAR Subpart 4.4, which requires the clause to be included in any contract when the contract may require access to classified information, were consistent with customary commercial practice for this contract and therefore incorporated FAR clause 52.204-2 and the DD Form 254 in the contract.[5] In addition, the contracting officer included supplemental

[2] FAR Part 12 prescribes policies and procedures unique to the acquisition of commercial items. FAR 12.000. "Commercial items" are generally defined as any item, other than real property, that is of a type customarily used by the general public or by non-governmental entities for purposes other than governmental purposes. FAR 2.101
[3] FAR 12.301(a)(1).
[4] FAR 12.301(a)(2).
[5] N00039-10-D-0010, Section C, clauses C-1 and C-2; N00039-10-D-0010 Attachment 5.

security requirements that are used by the Space and Naval Warfare Systems Command (SPAWAR) whenever a DD Form 254 is required.[6]

HPES issued several purchase orders to The Experts, Inc. (The Experts), for support of the CoSC beginning at the start of CoSC performance in September/October 2010. These purchase orders flowed down certain security requirements from the prime contract, including conformance with the NISPOM and the prime contract's Information Technology (IT) Systems Personnel Security Program Requirements and On-Site Security Requirements. The DD Form 254 for subcontractor The Experts identifies requirements for a top secret facility clearance. In addition, it includes the IT Systems Personnel Security Program Requirements and On-Site Security Requirements. The DD Form 254 for The Experts was approved by the HPES Facility Security Officer and by SPAWAR.

Recommendation 2 – Update Requirements for Contractors Reporting Adverse Information

- In addition to the requirements under the NISPOM that adverse information must be reported to the CSA and, if the cleared employee is employed on a Federal installation, to the commander or head of the installation, the NMCARS should be updated with a provision requiring that a contractor must notify the Security Officer for the head of the contracting activity regarding any adverse information. This is necessary to ensure that adverse information is diligently evaluated, that the CSA assesses the information in a timely manner, and that the DON promptly implements a risk assessment for continued physical and logical access to the facility and installation and IT system. ASN (RD&A) should assess whether the proposed NMCARS change should be incorporated into existing contracts.

- Further, the General Counsel and ASN (RD&A) should be directed to consider whether failure to report adverse information should be designated as a cause for debarment or a basis for termination for default of a specific contract. Any necessary change to acquisition regulations shall be proposed after this evaluation is complete.

- As part of the JAGMAN investigation, the Investigating Officer should:

    - Identify, and determine whether HPES and The Experts complied with, the applicable background investigation requirements for Alexis under The Experts's subcontract, including those required for security clearance reviews, routine physical access to a federally-controlled facility, and routine access to a federally-

[6] Contract clause C-1 "Security Requirements (Dec 1999) provides:

> The work to be performed under this contract as delineated in the DD Form 254, attachment 5 involves access to and handling of classified material up to and including __SCI__. In addition to the requirements of the FAR 52.204-2 "Security Requirements" clause, the Contractor shall appoint a Security Officer, who shall (1) be responsible for all security aspects of the work performed under this contract, (2) assure compliance with the National Industry Security Program Operating Manual (DODINST 5220.22M), and (3) assure compliance with any written instructions from the Security Officer [To be provided upon award].

controlled information system, as well as the criminal background check required under the subcontract.

- Evaluate the information available to the subcontractor, contractor, and Government officials regarding Alexis's behavior since being assigned to the CoSC, including the events that occurred in Newport, Rhode Island, in August 2013.
- Determine whether all applicable reporting requirements were complied with in relation to these events.
- Determine why The Experts debriefed Alexis from classified information on August 7, 2013, and re-indoctrinated him on August 9, 2013.
- Determine whether any adverse information notifications regarding Alexis were provided to the CSA or installation commander(s) based on events that occurred while he was performing work in support of Government contracts.
- If any adverse information reports were received, determine whether the appropriate procedures were followed and assessments made.

Background

Contractors are required to report adverse information regarding any of their cleared employees to the Cognizant Security Agency (CSA). NISPOM ¶ 1-302a. In the case of the CoSC and in accordance with the NISPOM, the CSA is the Defense Security Service (DSS). Adverse information includes any information that adversely reflects on the integrity or character of a cleared employee, that suggests that his or her ability to safeguard classified information may be impaired, or that his or her access to classified information clearly may not be in the interest of national security. NISPOM Appendix C. In addition, if the cleared contractor employee is employed on a Federal installation, the contractor is required to furnish a copy of the report and its final disposition to the commander or head of the installation. NISPOM ¶ 1-302a. Reports based on rumor or innuendo should not be made. *Id*. Reports of adverse information, as an initial matter, are intended to prevent unauthorized disclosure of classified information. NISPOM ¶ 1-100. The use of adverse information for other purposes, *e.g.*, identifying insider threats to the security of personnel and facilities from a continuous evaluation standpoint, is addressed by TAB C.

Application of Processes and Requirements to the CoSC Contract

In performance of the CoSC, HPES entered into subcontracts through purchase orders with The Experts for seat refresh/new seat delivery.[7] HPES Statement of Work for Subcontracting of Solutions and Projects, version #2, dated January 11, 2012 (HPES SOW), identifies the terms of the subcontracts with The Experts. Section 4.3 of this document provides that The Experts and its employees must at all times adhere to the security requirements of HPES and/or the Government as provided to The Experts by the HPES project manager. Government security badges, background checks, and/or drug testing may be required. The requirements with respect to background checks for security clearance eligibility are the same for military, civilian, and contractor personnel. In addition, when a contractor employee requires routine physical access to a federally-controlled facility, routine access to a federally-controlled information system, or

[7] Seats are end user computer devices, *e.g.*, desktop computers, laptop computers, etc.

access to classified materials, contractor employees are subject to background investigations that are similar to the general suitability and security determinations that are imposed on federal employees. The rapid review did not assess the extent to which the security clearance reviews and routine access reviews applied to Alexis under this subcontract.

In the addition to specific requirements such as those imposed for security clearance reviews and routine access, the terms of the contract control the level of background investigation required, if any. With respect to subcontractors under CoSC, Section 4.7 of the HPES SOW required The Experts to conduct a background check of all personnel prior to initial employment or prior to assignment to HPES. The manner and scope of the background check was a matter within the sole discretion of The Experts, provided that they included a criminal background check for the past seven years, including both felonies and misdemeanors for all jurisdictions where the personnel resided or worked. No personnel shall be assigned to the subcontract who have been convicted of a crime that was job-related or would present safety or security risks, and individuals with convictions for any of a number of delineated crimes, including crimes involving weapons, generally should not be placed at HPES. Considerations discovered during background checks that would be a potential business concern were required to be communicated to HPES before the person was used under the subcontract.

The Navy Yard shooter, Aaron Alexis, possessed a Secret security clearance. Alexis was granted access, both to the Navy Yard and to Building # 197, because he was an employee of an HPES subcontractor under the CoSC. The rapid review did not uncover the manner and scope of any background check that The Experts may have conducted on Alexis prior to assigning him to support the CoSC. The means by which The Experts conducted a criminal background check on Alexis, and any adverse information that may have been uncovered during that background check, are unknown at this time to the authors of this rapid review.

Furthermore, the subcontractor, The Experts, was required to report events that have an impact on the status of the facility clearance, the status of an employee's personnel clearance, the proper safeguarding of classified information, or an indication that classified information has been lost or compromised. This reporting requirement included any adverse information on an assigned employee's continued suitability for continued access to classified information. According to Alexis's Joint Personnel Adjudication System (JPAS) record, Alexis was debriefed by The Experts from access to classified information on August 7, 2013, and re-indoctrinated by The Experts on August 9, 2013. There is no additional information in his JPAS record to indicate why it was done.

On September 23, 2013, the contracting officer asked HPES to provide information on any adverse information report that HPES had provided to the Government under CoSC or that The Experts had provided to HPES under CoSC; and immediately notify the CSA of any adverse information regarding Alexis that had not been reported previously. On September 25, 2013, HPES severed its relationship with The Experts. On September 27, 2013, in response to the contracting officer's request, HPES informed the contracting officer that it had not received any adverse information reports on Alexis prior to the events of September 16, 2013; that the HPES Industrial Security Office did not receive any such reports regarding Alexis; and that HPES had not provided the Government with any information about Alexis at that time. In addition, HPES

notified the contracting officer of an internal investigation that the Hewlett-Packard Company (HP) initiated on September 16, 2013, after learning of the fatal shooting at the Navy Yard. Also on September 27, 2013, HPES provided the contracting officer with a copy of HP's interim report on the internal investigation. The interim report on HP's internal investigation was also submitted to the CSA and the Defense Security Service.

Recommendation 3 – Conduct an In-Depth Investigation of HPES' and its Subcontractors' Compliance with Previously Agreed-Upon Security Improvements

- The Naval Audit Service should be tasked to conduct a review of the CoSC, similar to the previous audit of the NMCI contract, in order to assess compliance of HPES and its subcontractors, as well as to assess DON internal controls. The Naval Audit Service should be tasked to notify the DON Acquisition Integrity office if it finds any compliance or internal control issues similar to those identified in the previous audit of the NMCI contract.

- ASN (RD&A) should be tasked to consult with the National Industrial Security Program Policy Advisory Committee (NISPPAC), a Federal advisory committee that advises the Director of the Information Security Oversight Office, National Archives and Records Administration, and industry to identify potential improvements to contractor personnel security processes and requirements. Such improvements, if any, should be incorporated into the NMCARS and forwarded to USD (AT&L) and the Under Secretary of Defense for Intelligence for appropriate action.

Background

It is noted that Electronic Data Systems, LL.C. (EDS), an HP company and predecessor to HPES, was the subject of a DON Acquisition Integrity Office (AIO) review in 2008-2009 under the predecessor Navy Marine Corps Intranet (NMCI) contract, based in part on subcontractor misuse of personally identifiable information. That incident involved a seat deployment subcontractor technician being permitted to work without the subcontractor completing the screening process required by its subcontract with EDS. It was also discovered that the same subcontractor had employed several persons who had criminal records. As a result, EDS stated that it had implemented enhanced screening requirements for subcontractor employees, flowed down security and other requirements to its subcontracts, audited subcontractor hiring and screening practices, and conducted other specific process improvements to strengthen its security processes on the NMCI contract. The screening requirements and flowdown of security and related requirements were incorporated by HPES in its CoSC subcontracts.

It is further noted that as a result of the AIO review, the Naval Audit Service conducted an audit which resulted in the report, "Controls Over Navy Marine Corps Intranet Contractors and Subcontractors Accessing Department of the Navy Information" dated 26 May 2011. The Naval Audit Service found that the NMCI Program Management Office did not perform periodic random inspections of the contractor or subcontractors, or otherwise institute an oversight mechanism, to ensure all personnel who required a security clearance or IT-level access had been properly cleared per DON policies. The Audit did not identify any systemic conditions related to

contractor non-compliance. In response to the Audit Report, the Program Executive Office-Enterprise Information Systems (PEO (EIS)) advised the Naval Audit Service in June 2011 that it would task the Defense Contract Management Agency to perform recommended surveillance actions and request that the Defense Security Service include HPES and associated subcontractors in its contractor site inspections and personnel security audits.

Eligibility for Clearance:
Process, Policy, and Recommendations

Background

All Department of the Navy (DON) employees – civilian and military (active and reserve) – are subject to and undergo some kind of background investigation as part of the entrance to service or hiring process to determine *suitability* for employment.[1] As we know from our review of Navy, DON Central Adjudication Facility (DONCAF), and Department of Defense Consolidated Adjudication Facility (DODCAF) records[2], Aaron Alexis underwent an Entrance National Agency Check in March 2007 per a request from the Navy's Military Entrance Processing Command. The Office of Personnel Management (OPM) conducted his Navy enlistment *suitability* check from March 22, 2007, to April 6, 2007. The check included:

- Defense Central Index of Investigation (DCII);
- FBI Investigations Records (Name Check);
- FBI Fingerprint Check; and
- OPM Security/Suitability Investigations Index;

Aaron Alexis then underwent a National Agency Check with Law and Credit Check investigation (NACLC) from April 9 to August 24, 2007, to determine whether he was suitable for access to sensitive and classified information. This investigation included the checks listed above and the following additional checks:

- Credit check;
- Local agency check (law enforcement); and
- Investigation to resolve specific issue (subject interview).

Based on the fingerprint check with the FBI's Criminal Justice Information System and residences listed in Alexis's Standard Form 86 (SF 86–National Security Questionnaire), OPM's investigation included statewide criminal checks in New York and Washington. There were no criminal related records found for the state of New York. There was a malicious mischief arrest found in the FBI fingerprint check and the statewide district and municipal courts records check in the state of Washington. Due to Alexis's omission of that information on his SF 86, OPM exercised the option to conduct a subject interview with Alexis. Since the Washington statewide check did not reflect that a firearm was used, the resulting report to the DONCAF did not include any mention of the use of a firearm in the malicious mischief incident.

[1] Suitability is defined in 5 CFR Section 731 as an action that determines fitness for employment.
[2] The Department of the Navy's Central Adjudication Facility (DONCAF) was integrated into the DoD Consolidated Adjudication Facility (DODCAF) on 27 Jan 13. WNY TF Part 1: Timeline of Events Concerning Aaron Alexis, dtd September 20, 2013.

The Clearance Process

The three steps in the clearance process include initiation, investigation, and adjudication. Initiation requires the individual to provide personal information on their family and associates; employment; military service; residences; references; drug and alcohol use; foreign activities, associations, contacts, and travel; association record; credit; criminal; and mental health history. This is the employee's first opportunity to disclose fully information required by the Government. Aaron Alexis completed a SF 86 during the initiation of his NACLC background investigation. The unit, command or Command Security Manager will assist the employee and is responsible for releasing the completed SF 86 to OPM.

The investigation is the second step in the clearance process. Upon receipt of the SF 86, OPM, as required by the Federal Investigative Standards[3], conducts the investigation. OPM has been the primary investigative service provider for the Department of Defense (DoD) since 2005. OPM has prescribed timelines to conduct the investigation.[4] At the time of Aaron Alexis's investigation, OPM had 90 days to complete the NACLC investigation described above.

The third step in the clearance process is adjudication. OPM submits the SF 86 and their investigation report to an adjudication facility such as the DODCAF. Trained and certified adjudicators use the 13 Federal adjudicative guidelines[5] to determine whether a person is reliable, trustworthy and suitable to occupy a national security position. It involves the careful weighing of variables under what is known as the "whole-person concept." Any doubt concerning suitability for access to sensitive or classified information is resolved in favor of national security.

In evaluating an individual's negative conduct, the adjudicator considers the following factors, per the adjudicative guidelines:

- Nature, extent, and seriousness of the conduct;
- Circumstances surrounding the conduct, to include knowledgeable participation;
- Frequency and recency of the conduct;
- Individual's age and maturity at the time of the conduct;
- Extent to which participation is voluntary;
- Presence or absence of rehabilitation and other permanent behavioral changes;
- Motivation for the conduct;
- Potential for pressure, coercion, exploitation, or duress; and

[3] The Federal Investigative Standards have been updated three times (29 Jul 1997, 13 Dec 2008, and Dec 2012) since President Clinton signed EO 12968: Access to Classified Information in August 1995.
[4] *The Intelligence Reform and Terrorism Prevention Act of 2004*, directed that at least 80% of investigation had to be completed within 90 days of receipt beginning in Dec 2006. It also stipulated that by Dec 2009 at least 90% of investigations had to be completed within 40 days of receipt.
[5] Federal Adjudicative Guidelines were established by EO 12968 dtd 4 Aug 1995 and revised on 29 Dec 2008.

- Likelihood of continuation or recurrence.

The adjudication facility will only determine ***eligibility for access*** to sensitive and/or classified information. Based on a favorable adjudication eligibility determination, a Secret clearance is valid for 10 years, and Top Secret is valid for 5 years. The ***granting of access*** to classified information is determined by the commander, director, or supervisor. In the case of Aaron Alexis, his command, Fleet Logistics Squadron VR-46, never accessed him to classified information. Figure 1 provides a flow chart of the clearance process.

Contractors working on federal contracts are subject to the same investigative and adjudicative guidelines as federal employees. The only difference is that the contractor's facility security officer submits an individual's SF 86 via the Defense Security Service's Personnel Security Management Office–Industry to OPM.

The following are the relevant current Federal, DoD, and DON personnel security policies:

- EO 10450 – Security Requirements For Government Employment (April 27, 1953);
- EO 12968 – Access to Classified Data (August 4, 1995);
- EO 13467 – Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information (July 2, 2008);
- EO 13526 – Classified National Security Information (December 29, 2009);
- DoD Directive 5200.2R – Personnel Security Program *(updated: February 23, 1996)*;
- SECNAV Manual 5510.30 – Personnel Security Program (June 2006); and
- SECNAVINST 5510-30b – Personnel Security Program (October 6, 2006).

Per SECNAV Manual 5510.30, Exhibit 10A, commanders are required to report the following using the Joint Personnel Adjudication System (JPAS) in support of a Continuous Evaluation[6] process:

- Involvement in activities or sympathetic association with persons which/who unlawfully practice or advocate the overthrow or alteration of the U.S. by unconstitutional means.
- Foreign influence/concerns/close personal association with foreign nationals or nations.
- Foreign citizenship (dual citizenship) or foreign monetary interests.
- Sexual behavior that is criminal or reflects a lack of judgment or discretion.

[6] Continuous Evaluation is defined in EO 13467 as reviewing the background of an individual who has been determined to be *eligible* for access to classified information (including additional or new checks of commercial databases, Government databases, and other information lawfully available to security officials) at any time during the period of eligibility to determine whether that individual continues to meet the requirements for *eligibility* for access to classified information.

- Conduct involving questionable judgment, untrustworthiness, unreliability or unwillingness to comply with rules and regulations, or unwillingness to cooperate with security clearance processing.
- Unexplained affluence or excessive indebtedness.
- Alcohol abuse.
- Illegal or improper drug use/involvement.
- Apparent mental, emotional or personality disorder(s).
- Criminal conduct.
- Noncompliance with security requirements.
- Engagement in outside activities that could cause a conflict of interest.
- Misuse of information technology system.

All contractors employed under a federal classified contract are subject to the same Continuous Evaluation requirements as federal employees and military members. A company's facility security officer, like any security manager in federal employment, is required to report any conduct that meets the criteria above to the DSS Personnel Security Management Office-Industry.

Recommendations

The review of current personnel security policy relevant to eligibility for clearance or access to classified or sensitive information reveals three primary weaknesses:

- DoDD 5200.2R requires self-reporting but is outdated and focused primarily on espionage.
- Although SECNAV Manual 5510.30 directs cleared *individuals* to be aware of personnel security standards and requires them to report information that meets Continuous Evaluation criteria, self-reporting is unreliable.
- Similarly, while DoDD 5200.2R and SECNAV Manual 5510.30 require *supervisors* and *co-workers* to report observations of incidents that meet Continuous Evaluation criteria, in practice, such incidents are rarely reported.

There is a delicate balance between central policy guidance and local level execution based on the conditions in the unit, command, or organization. For example during the interview with Aaron Alexis's last Commanding Officer (CO), it was clear that the CO was aware of JPAS as a tool to report security-related incidents.[7] However, given that Alexis was not accessed to sensitive or classified information, given that Alexis's issues were characterized as performance-related and not personnel security related, and given that Alexis's stated intention was to use the

[7] Interview of CAPT (b) conducted by ASN M&RA on September 19, 2013.

GI Bill benefits to return to school upon release from active duty, the CO did not report them via JPAS.

Given the facts ascertained to date and given the policies and processes in place today, this rapid review recommends the following actions:

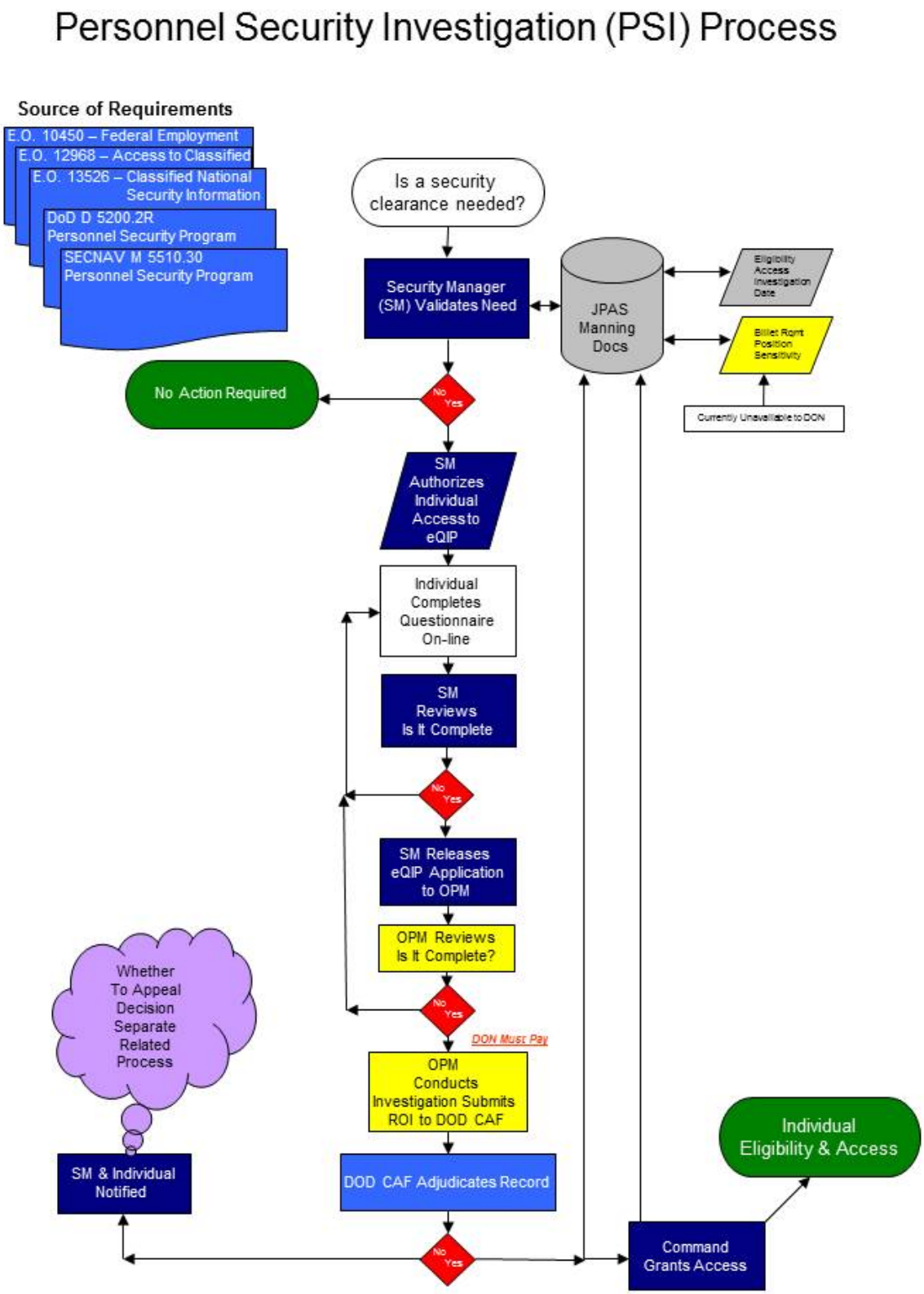
- DUSN PPOI should be directed to prepare an ALNAV for SECNAV's signature directing a personnel security review for all DON employees. The ALNAV would direct all DON employees to familiarize themselves with the Continuous Evaluation self-reporting criteria in SECNAV M-5510.30. Additionally, it would direct all commanding officers, supervisors, and security managers/officers to conduct a thorough review of command records to ensure that any incidents occurring during a service member's assignment at the current command, meeting the Continuous Evaluation reporting criteria, have been properly documented in JPAS. After a deliberate and complete evaluation of all incidents, if any meet the reporting criteria, command security managers will have 30 days from the issuance of the ALNAV to report the incidents in JPAS.
- DUSN PPOI should be directed to update SECNAVINST 5510.30B and SECNAV M-5510.30 to require the Command Security Manager responsibilities be assigned to an individual who has unfettered access to the unit's leader, whether military or civilian, and who has command-wide insight into all personnel-related events. At the individual unit level, where the Command Security Manager is often a collateral duty, this should most likely be the Executive Officer or Senior Enlisted Advisor, rather than a junior officer or enlisted member.
  [***Directed by SECNAV on September 24, 2013***]
- SECNAV recommend, via the Secretary of Defense, to the Director of National Intelligence, as the Federal Security Executive Agent [8], the following suggestions for improvement:
  - Require all OPM investigative reports include any available original police documents related to the subject being investigated for clearance eligibility. [***Completed: SECNAV memo to SECDEF, September 24, 2013***]
  - Change federal standards and policy to create a requirement to inactivate those individuals who have eligibility but not accessed to classified information immediately upon departure from government service (military, civilian, and contractor). Upon return to government service of any kind, a NACLC investigation, with the appropriate adjudication, would be required before eligibility would be restored.[9]
  - Change federal standards and policy to create a requirement to inactivate those individuals who have eligibility and accessed to classified information upon departure from government service (military, civilian, and contractor) when the break in service is more than 90 days. Upon return to government service of any

[8] EO 13467 established the Director of National Intelligence as the federal Security Executive Agent.
[9] According to a recently released cost schedule from OPM, the cost of a NACLC investigation will be $210 in FY14.

kind, a NACLC investigation, with the appropriate adjudication, would be required before eligibility would be restored.

- DUSN PPOI should be directed to ensure the initiation of an automated Continuous Evaluation capability for DON employees. The first step would be to accelerate and resource the Defense Security Enterprise's Continuing Evaluation Concept Demonstration (CE CD). The CE CD will build upon a successful 2012 Army Continuous Evaluation pilot covering ~3,400 employees with recently completed and adjudicated background investigations, which discovered, using regular queries against existing databases, that 22% of the pilot population had reportable security incidents that were not self-reported.

Figure 1.


Personnel Security Investigation (PSI) Process
Source of Requirements
E.O. 10450 – Federal Employment
E.O. 12968 – Access to Classified
E.O. 13526 – Classified National Security Information
DoD D 5200.2R Personnel Security Program
SECNAV M 5510.30 Personnel Security Program
Is a security clearance needed?
Security Manager (SM) Validates Need
JPAS Manning Docs
Eligibility Access Investigation Date
Billet Rqmt Position Sensitivity
Currently Unavailable to DON
No Action Required
No
Yes
SM Authorizes Individual Access to eQIP
Individual Completes Questionnaire On-line
SM Reviews Is It Complete
No
Yes
SM Releases eQIP Application to OPM
OPM Reviews Is It Complete?
No
Yes
DON Must Pay
OPM Conducts Investigation Submits ROI to DOD CAF
DOD CAF Adjudicates Record
No
Yes
Whether To Appeal Decision Separate Related Process
SM & Individual Notified
Command Grants Access
Individual Eligibility & Access